UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,600	07/26/2001	Chris A. Barton	NAI1P020/01.139.01	8707

28875 7590 07/27/2009

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
07/27/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

anita@zilkakotab.com
erica@zilkakotab.com
dottie@zilkakotab.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CHRIS A. BARTON, JAMES M. VIGNOLES, and JAMES W. LAWRENCE

Appeal 2009-001730
Application 09/916,600
Technology Center 2400

Decided:[1] July 24, 2009

Before HOWARD B. BLANKENSHIP, JOHN A. JEFFERY, and DEBRA K. STEPHENS, *Administrative Patent Judges*.

STEPHENS, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from a final rejection of claims 1, 2, 4-7, 10-18, 20-23, and 26-43 under 35 U.S.C. §103(a) and claims 17, 18, 20-23, 26-32, 34, and 39 under 35 U.S.C. §101. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

Introduction

According to Appellants, the invention is a system and method directed to scanning data to identify data passing to and from storage for any malicious code (Spec. 1, Field of the Invention).

Exemplary Claim(s)

Claims 1, 17, 20, and 34 are exemplary claims and are reproduced below:

1. A method for scanning data read from storage, comprising:
a) receiving a request for a data saved in storage from a central processing unit;
b) scanning the requested data for malicious code; and
c) transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning;
wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;
wherein a user is allowed to disable the scanning module, and a data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

17. A computer program product for scanning data read from storage, comprising:

a) computer code for receiving a request for data saved in storage from a central processing unit;

b) computer code for scanning the requested data for malicious code; and

c) computer code for transmitting the data from the storage to the central processing unit if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed the disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module.

20. The computer program product as recited in claim 17, wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough.

34. A computer program product for scanning data written to storage, comprising:

a) computer code for receiving a request for data to be written in storage, the request being received from a central processing unit;

b) computer code for scanning the data for malicious code; and

c) computer code for writing the data to the storage if malicious code is not found in the data during the scanning;

wherein the scanning is performed by a scanning module coupled to a storage subsystem controller;

wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module.

Prior Art

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Makita	US 2001/0007120 A1	Jul. 5, 2001
Browne	US 6,272,533 B1	Aug. 7, 2001 (filed Feb. 16, 1999)
Flint	US 6,735,700 B1	May 11, 2004

Rejections

The Examiner rejected claims 1, 2, 4-7, 10-18, 20-23 and 26-40 under 35 U.S.C. § 103(a) as being unpatentable over Makita and Flint.

The Examiner rejected claims 41-43 are rejected under 35 U.S.C. § 103(a) as being obvious over Makita, Flint, and Browne.

The Examiner rejected claims 17, 18, 20-23, 26-32, 34, and 39 under 35 U.S.C. § 101 as being directed to non-statutory matter.

Claims 3, 8, 9, 19, 24, and 25 have been cancelled.[2]

Rejections under 35 U.S.C. § 103(a)

Appellants' Contentions

[2] The Examiner rejected claims 42 and 43 under 35 U.S.C. § 112, first paragraph; however, the Examiner has withdrawn this rejection as indicated in the Examiner's Answer (Ans. 17, § (10), Issue #1).

We note claim 26 depends from claim 19; however, claim 19 has been cancelled. Claim 19 depended upon claim 17 and thus, we treat claim 26 as being dependent upon claim 17 for the purposes of this Appeal.

Appellants argue Flint discloses that a user terminates the anti-virus program and not that when the scanning module is disabled, data is precluded from being transmitted from the storage to the central processing unit (App. Br. 13, § VII., Issue #2, Group #1). Additionally, Appellants contend Makita does not teach what occurs, when no virus check is performed – Makita only teaches what happens when the virus check finds the presence or non-presences of a virus (App. Br. 14, § VII, Issue #2, Group #1). Thus, Appellants argue, neither of the prior art references, when taken alone or in combination, teaches that data is precluded from being transmitted from the storage to the central processing unit, when the scanning module is disabled (*id.*).

Examiner's Findings

The Examiner finds Flint teaches disabling a virus scanner and when the virus scanner is stopped, invalidating the session stamp of the file (Ans. 18, § (10), Issue #1, Group #1). The Examiner then finds the session stamp is checked to determine whether the stamp is valid or not and if not, the file is scanned for viruses (*id.*). Then, according to the Examiner's findings, the session stamp is updated to indicate it is invalid, since the virus scanner is stopped at this point (*id.*). Additionally, the Examiner finds the virus scanning program is stopped without updating the session stamp to indicate it is valid; therefore, this step will continue to be repeated as long as the virus scanner is off (*id.*). Thus, the Examiner finds the session stamp will never be validated and the file cannot be accessed (*id.*).

Issue

Have Appellants met the burden of showing the Examiner erred in finding Flint teaches that, when the scanning module is disabled, data is prevented from being transmitted from the storage to the central processing unit (CPU)?

FINDINGS OF FACT (FF)

Appellants' Invention

(1) Appellants' invention is directed to a system, method, and computer program product for scanning data that a central processing unit (CPU) requests and for transmitting the data only if no malicious code is found (Spec. 3, ll. 3-7). Appellants' invention is further directed to a system, method, and computer program product for scanning data requested to be written to storage and if no malicious code is found, writing the data to storage (Spec. 3, ll. 7-9).

(2) Scanning may be performed by a scanning module (that may include hardware and/or software) located in a storage subsystem (Spec. 3, ll. 16-20). The storage subsystem controller may take any form including hardware, software, or any other type of logic (Spec. 5, ll. 21-24).

Makita's Invention

(3) Makita relates to a storage device connected to a host computer that stores information processed in the host computer to reduce the processing load of the host computer (Abstract). The external storage 410 is a recording and/or reproduction device includes a compression and

expansion unit 411, a virus check unit 413, an interface unit 21, a storage unit 22, a memory 212, and a file management unit 211 (pg. 7, [0168]; Fig. 15).

(4) The virus check unit performs a virus check on information to be recorded on a recording medium (pg. 7, [0174]; Fig. 16).

Flint's Invention

(5) Flint is directed to fast virus scanning performed by creating a unique session key, when anti-virus software is executed, and a session stamp for each file is scanned during that execution (Abstract). The session stamp is associated and stored with the scanned file (*id.*). When a request for the file is made, the session key is used to validate the session stamp (*id.*). An invalid or absent session stamp indicates the file needs to be scanned (*id.*).

(6) When executed, the anti-virus method 400 generates a current session key (block 401) (col. 8, ll. 59-60; Fig. 4). Three main activities that operate in parallel are initiated: pre-population scan (block 403), monitoring of activity in the file system (block 407), and waiting for user input (block 421) (col. 8, ll. 60-63, 65-67; col. 9, ll. 5-7; Fig. 4).

(7) The file system monitoring activity (block 407) checks to determine if a file is accessed (block 409), and if the anti-virus scanning facility of the method is active (block 411) (col. 8, l. 67 – col. 9, l. 3). When the file is accessed, if the anti-virus scanning facility is active, the method 400 performs an on-access scan process; if the anti-virus scanning facility

has been stopped, the session stamp of the file is invalidated (block 415) (col. 8, l. 67 - col. 9, l. 4; Fig. 4).

(8) The user input activity (block 421) checks to see if the user input specifies the termination of the anti-virus program (block 427), and if so, a termination process (block 429) is performed (col. 9, ll. 5-13).

(9) When the anti-virus program 400 is terminated (block 427), if configured by the user, the "most recently used" (MRU) files for use by the pre-population scan method (block 801) in cache are saved to non-volatile storage (block 803) (col. 9, ll. 31-38; Fig. 8).

(10) In an alternate embodiment, when a file is accessed while the anti-virus scanning facility is inactive (block 411), the file can also be added to a rescan list in addition to having its session stamp invalidated at block 415 (col. 9, ll. 25-28) . When the user requests that the scanning be resumed (block 431), the rescan list is used as the file set for the on-demand scan method (col. 9, ll. 29-30).

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

ANALYSIS

Claims 1, 2, 4-7, 10-18, 20-23 and 26-40

Flint teaches disabling the anti-virus program and invalidating the file's session stamp when the virus scanner is disabled (FF 5 and FF 7). However, we find Flint does not teach what happens when the anti-virus program 400 is terminated and only teaches that, as shown in Figure 8, if a user chooses, the MRU cache is written to permanent storage before termination. *See* FF 9.

Although Flint teaches that the session stamp is invalidated, we find Flint does not teach what the system does, if the session stamp is invalid and is unable to scan the file for viruses (Fig. 4, circle 4; Fig. 6, blocks 611, 607). We further find that Flint does not teach that when the anti-virus scanning is terminated, the data in storage is prevented from being transmitted to/from the CPU. Instead, we find Flint teaches the session stamp is invalidated to indicate the file needs to be scanned.

Therefore, we find neither Flint nor Makita, taken alone or in combination, teaches or suggests that when the anti-virus scanning is disabled, the data in storage is prevented from being transmitted to the CPU from storage. We further find neither Flint nor Makita, taken alone or in combination, teaches or suggests that when the anti-virus scanning is disabled, the data in the CPU is prevented from being transmitted to the storage.

For the foregoing reasons, Appellants have persuaded us of error in the Examiner's obviousness rejection of independent claim 1 and independent claims 17, 33, 34, 35, and 39 which recite commensurate limitations. Accordingly, we will not sustain the Examiner's rejection of

those claims and dependent claims 2, 4-7, 10-16, 18, 20-23, 26-32, 36-38, and 40 for similar reasons.

Claims 41-43

In addition, we further find Browne does not cure the deficiencies of Flint and Makita, taken alone or in combination. Specifically, we find none of the references, Makita, Flint, Browne, taken alone or in combination teaches or suggests that when the anti-virus scanning is disabled, data is prevented from being transmitted between the storage and the CPU. Accordingly, we will not sustain the Examiner's rejection of claims 41-43.

CONCLUSION

Appellants have met the burden of showing the Examiner erred in finding Flint teaches that when the scanning module is disabled, data is prevented from being transmitted from the storage to the central processing unit (CPU).

Rejections under 35 U.S.C. § 101

Appellants' Contentions

Appellants argue their recited "computer program product for scanning data read from storage" as recited in claim 17 is an article of manufacture (Reply Br. 18, Issue # 5, Group # 1). Appellants further argue their invention, by virtue of "transmitting" data and scanning the "requested data" performs a "transformation" of an article or physical object to a

different state or thing (Reply Br. 19, Issue # 5, Group # 1). Additionally, Appellants argue claim 34 recites computer code for "writing" data, and thus again performs a "transformation" (Reply Br. 20, Issue # 5, Group # 2).

As to claim 39, Appellants further argue "means for controlling access to the data saved therein," "means for issuing read requests for reading the data saved therein for processing purposes," and "means for . . . scanning the data for malicious code in response to the requests," all produce a "transformation" (Reply Br. 20-21, Issue # 5, Group # 3). Additionally, Appellants argue the claimed invention clearly recites "a useful feature that provides real-world results which can be substantially repeatable or substantially produce the same result again" (Reply Br. 22, Issue # 5, Group # 3).

Examiner's Findings

The Examiner concludes claims 17, 18, 20-23, 26-32, 34 and 39 recite non-statutory subject matter, since the claims relate to a computer program product that is computer code (Ans. 17, § Grounds of Rejection, ¶ New Grounds of Rejection). Additionally, the Examiner finds claim 39 recites a system with different means plus function language and looking to the specification, finds the "means" can be software (*id.*). Therefore, the Examiner concludes, the claims do not recite a machine or article of manufacture or any other statutory subject matter, but are at best, functional descriptive material per se (*id.*).

Issue

Have Appellants met the burden of showing the Examiner erred in concluding claims 17, 18, 20-23, 26-32, 34, and 39 recite non-statutory subject matter?

FINDINGS OF FACT (FF)

Appellants' Invention

(11) A central processing unit may be a microprocessor interconnected via a system bus to other units (Spec. 6, ll. 26-29).

(12) Storage may include a hard drive, compact disc-read only memory (CD-ROM), a floppy disk, and/or any other type of device capable of storing data (Spec. 5, ll. 19-21).

PRINCIPLES OF LAW

"A transitory, propagating signal . . . is not a 'process, machine, manufacture, or composition of matter.' Those four categories define the explicit scope and reach of subject matter patentable under 35 U.S.C. § 101." *In re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007), *reh'g denied en banc*, 515 F.3d 1361 (Fed. Circ. 2008), *cert. denied*, 129 S. Ct. 70 (2008). "If a claim covers material not found in any of the four statutory categories, that claim falls outside the plainly expressed scope of § 101 even if the subject matter is otherwise new and useful." *Id.* at 1354.

ANALYSIS

Claims 17 and 34

Claim 17 recites a computer program product comprising computer code. We start with determining the scope of claims 17 and 34, since claim construction is "an important first step in a § 101 analysis." *In re Bilski*, 545 F.3d 943, 951 (Fed. Cir. 2008) (en banc), *cert. granted*, 77 U.S.L.W. 3442, 3653, 3656 (U.S. June 1, 2009) (No. 08-964). Each of these claims recites a computer program product for scanning data read from storage. The structures that are encompassed by the computer program product in claims 17 and 34, however, are vast. Appellants have not defined or discussed the phrase "computer program product" in their Specification. Giving claims 17 and 34 and the phrase "computer program product" the broadest reasonable interpretation in light of the Specification, these claims are broad enough to encompass a signal.

We additionally find the recitation of "storage" in claims 17 and 34 does not provide structure either. Specifically, we find the storage does not further limit the "computer program product" but is instead, a description of from where the data has been read. Thus, we find the storage does not add any structure to the recited "computer program product."

Since "computer program product" can be signals and signals are not statutory subject matter, we conclude claims 17 and 34 cover at least one embodiment directed to non-statutory subject matter – a signal. Therefore, we conclude claims 17 and 34 are directed to non-statutory subject matter (claims which are broad enough to read on statutory as well as non-statutory subject matter are treated as unpatentable because an applicant can always amend the claims to limit them to statutory subject matter, such as a tangible

medium. *Cf. Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1330 (Fed. Cir. 2003); *see also* MPEP § 2105).

Claims 18-23 and 26-32

Claims 18, 20-23 and 26-32 do not further limit the computer program product. Claim 18 recites types of storage; however, as discussed above, the recitation of storage in claim 17 does not add structure. Since claim 18 only recites the types of storage, we find the additional limitation recited in claim 18 does not add structure. Similarly, the recited accessibility of storage recited in claim 32 does not add structure to the computer program product.

We additionally find claim 22 does not add structure since the recited scanning module is not the structure of the computer program product, but instead is what the computer program product is written to accommodate. Claims 26 and 28 recite additional computer code and thus, add no structure to the computer program product.

Claim 27 further limits the event, but still does not add structure; claim 29 recites the desired result once the computer program product is executed and thus does not add structure; and claims 31 and 32 recite what the computer code is written to perform – but again, does not add structure to the computer program product.

Claim 20 recites the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit; claim 21 recites the storage controller is coupled to the storage; and claim 23 recites

the scanning module includes hardware. Although each of these claims recites structure, the recited limitations are not the structure of the computer code. Instead, these recitations recite what the computer code is written to accommodate. For example, the computer code scans the requested data (as recited in claim 17). To write the computer code to perform this function, the code must be written to accommodate the specific structure of the system; however, this does not add structure to the code itself.

Thus, giving these claims their broadest reasonable reading, we conclude claims 18, 20-23 and 26-32 cover at least one embodiment directed to non-statutory subject matter. Accordingly, we conclude claims 18-23 and 26-32 do not recite statutory subject matter.

Claim 39

Lastly, claim 39 recites a system for scanning data read from storage. Claim 39 further recites this system includes various "means." Appellants state one of these means, "means for saving data therein", corresponds to item 202 of fig 2 – labelled as storage (App. Br. 9, § V.). Appellants have defined storage as a hard drive, compact disc-read only memory (CD-ROM), a floppy disk, and/or any other type of device capable of storing data (FF 12).

A machine has been defined by our Supreme Court as "a concrete thing consisting of parts, or of certain devices and combination of devices. This 'includes every mechanical device or combination of mechanical powers and devices to perform some function and produce a certain effect or result'" (*See In re Nuijten*, 500 F.3d 1346, 1357 (Fed. Cir. 2007), *reh'g*

denied en banc, 515 F.3d 1361 (Fed. Circ. 2008), *cert. denied*, 129 S. Ct. 70 (2008) (citations omitted)). Therefore, we find the recited storage is a machine.

Accordingly, since claim 39 recites storage which is a machine, we conclude claim 39 provides structure for a machine, and therefore, is directed to statutory subject matter.

CONCLUSION

We conclude Appellants *have not* met the burden of showing the Examiner erred in concluding claims 17, 18, 20-23, 26-32, and 34 recite non-statutory subject matter.

We conclude Appellants *have* met the burden of showing the Examiner erred in concluding claim 39 recites non-statutory subject matter.

DECISION

The Examiner's rejection of claims 1, 2, 4-7, 10-18, 20-23 and 26-40 under 35 U.S.C. § 103(a) as being unpatentable over Makita and Flint is reversed.

The Examiner's rejection of claims 41-43 are rejected under 35 U.S.C. § 103(a) as being obvious over Makita, Flint, and Browne is reversed.

The Examiner's rejection of claims 17, 18, 20-23, 26-32, and 34 under 35 U.S.C. § 101 as being directed to non-statutory subject matter is affirmed.

The Examiner's rejection of claim 39 under 35 U.S.C. § 101 as being directed to non-statutory subject matter is reversed.

"Notwithstanding any other provision of this paragraph, the failure of appellant to separately argue claims which appellant has grouped together shall constitute a waiver of any argument that the Board must consider the patentability of any grouped claim separately." (*See* 37 C.F.R. § 41.37(c)(1)(vii)).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

erc

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE CA 95172-1120